CCPA Guideline

Baseline information to help with CCPA compliance

Over the past year, the upcoming California Consumer Protection Act (CCPA) has been put under the spotlight as the first major legal foray into digital privacy and protection within the United States. Given the importance of California and its economy, not just within the US itself, but the global marketplace as buoyed by some of the biggest tech companies in the world. Often seen as a somewhat counterpart to the European Union enactment of the General Data Protection Regulation (GDPR), in actual fact, there are some key variations between CCPA and GDPR, largely due the genesis of CCPA and the drivers, whether it was the constant barrage of data breaches by major US companies, or the bringing to light of how social media and search information is used. Although many companies have already adopted privacy processes and procedures consistent with GDPR, the CCPA contains a number of variations that customers and end-users alike should be aware of.

The Episerver Customer-Centric Digital Experience Platform are ready today to help customers be CCPA compliant, as we have done for GDPR compliance since early 2018. Episerver continues to lead the industry with extensive expertise in protecting data, defending privacy, and complying with complex regulations. We believe that the CCPA is an important step forward for not just enabling individual privacy rights in California, but also a driver to ensuring more secure and protected online engagements throughout the US. We are prepared to help customers focus and expand on their core business through the most customer-centric digital experience platform available, while efficiently preparing for the CCPA.

Our commitment to GDPR compliance across our Cloud services has put us in great shape to support CCPA, but we have and will continue to drive towards continuous improvement and enablement of our customers to be successful and compliant.

Episerver has created these guides as baseline information to help Customers and Prospects understand not only the general challenges and opportunities there are with CCPA compliance, but also how the Episerver Customer-Centric Digital Experience Platform can be a key component of getting there.

CCPA Requirements for Consumer Rights

CCPA contains many requirements about collecting, storing, and using personal information, including:

- **Individuals have the right to be informed as to the personal data collection occurring**
- **Right to opt-out of consumer's personal information sale by a company to 3rd parties**
- **Right not to be discriminated against by a business for exercise of consumer rights**
- **The right to request information**
- **Direct right of action where a breach involved nonencrypted or nonredacted personal information (not cured within 30 days)**

For those that did not have to be GDPR compliant previously (for example, those organizations that do no interact with European Union individuals and/or organizations), these measures may require much more operational and process changes within the organization itself, in order to support CCPA. It is imperative that organizations review privacy and data management practices now, pick the right platform for compliance now adapt towards the future, and embrace "data protection and privacy by design".

Failure to comply with CCPA could prove costly, as companies that do not meet the requirements and obligations could face substantial fines and reputational harm (up to $7,500 per incident/customer data breached, or if you wanted to use Facebook's Cambridge Analytica incident, with Facebook's ~24.6 million users in California,. were Facebook found to have violated the CCPA, it could face a rough full maximum penalty of $61.6 billion for an unintentional violation affecting each of its users and up to $184.7 billion for an intentional violation).

10 first steps in your journey to CCPA compliance

Episerver products and services provide powerful solutions to help tackle these steps in a company's journey to compliance with CCPA, as it did with GDPR. These 10 topics discuss some of the high-level points of the CCPA, offer some personal thoughts on how organizations can best prepare and how Episerver is best positioned to enable all customers to reach their CCPA compliance and business goals. Please note, these are just my personal opinion, and do not represent formal legal advice on the matter.

1. Are you subject to the law?

Probably the first question your organization needs to answer - not every organization is subject to the CCPA. CCPA applies to businesses that buy, receive, or sell the personal information of 50,000 or more consumers, households, or devices; businesses that derive 50 percent or more of their annual revenue from selling consumers' personal information; or those that have gross annual revenues greater than $25 million. For-profit companies do not necessarily have to be based in California to be subject to the statute.

2. Establish a subject data request process.

While CCPA is not as stringent as GDRP in this regard, the verification obligations under CCPA are still significant. Treated much in the way GDPR subject access requests, organizations must be prepared to intake and effectuate consumer access and deletion requests as they come in.

Remember that businesses that fail to comply with those requirements and release personal information to the harm of the consumer may face litigation for those mistakes as well as other regulatory enforcement actions. Platforms like Episerver's Customer Centric Digital Experience Platform are developed with data protection and privacy in mind, with cloud services built around enabling customer to comply with requests, and where needed, Episerver assistance on such matters.

3. Data Mapping is key.

Again, in similar advice under GDPR, data mapping of the personal information that your organization maintains or that platforms like the Customer Centric Digital Experience Platform maintain on your behalf is imperative in enabling not just best practices on data protection, but also helping you quickly and efficiently deal with subject data requests. Organizations should know the types of personal information that have been collected in at least the past twelve (12) months, the purposes for which it was collected, and who (including the types) of entities such data was shared with, all tracked on an ongoing basis.

Note – there is a departure from GDPR here – CCPA also covers "offline" data as CCPA regulations clearly push data privacy disclosures into offline interactions, which includes onsite/in-store consumer interactions.

4. Revising online privacy notices and cookie banners.

CCPA puts a very definite onus on organizations to make sure that all online interactions (whether it be via website, mobile or otherwise), include descriptions of the categories of data and information collected, third parties with whom data is shared with, the rights available to individuals, and how to execute those rights under CCPA. While CCPA has clear requirements around giving the ability to individuals to opt-out of data collection (rather than GDPR's opt-in requirement), remember that tracking verifiable consent of the individual starts with giving them proper notice and ways to action their rights through an organization's privacy notices.

An often-missed area, (as with GDPR), is an organization's internal privacy policy as well as it's externally facing one. Internal privacy policies are those that are non-public facing

typically aimed at your employees, consultants and other working organizations. The same data description and use as described above should be scribed and put into process as well. Remember that any policy should be drafted with the specific needs and uses of the organization in mind to ensure that it is useful, implementable and most importantly enforceable. Note – here too, a departure from GDPR is the likely need to update/enable your cookie banners for online interaction. Episerver's support of such cookie management policies can enable quick adoption and modification as needed.

5. What is "reasonable security" practices and how do you conform?

CCPA contains security provisions on data protection and provides a private individual's right of action for consumers affected by a data breach caused by an organization's failure to provide 'reasonable security'. Remember too that this security requirement will be one of the first immediately enforceable acts on Jan. 1, 2020, either by the California Attorney General or via a private right of action.

Organizations should review information security practices and processes against established data security standards such ISO 27001, and digital platforms chosen, like the Episerver Customer Centric Digital Experience Platform, must at a minimum be certified against such standards. Organizations themselves should ensure appropriate documentation of any data controls is in place to demonstrate 'reasonable security', especially as evidentiary and roadmap to assist in the event of data breach.

6. You are your vendor's keeper.

Picking the right vendors for any engagement in the collection, processing or storage of personal information is key. As noted above, your vendors and platforms should enable industry-best data protection and privacy compliance and certifications, such as Episerver's Customer Centric Digital Experience Platform, to enable your own organization's overall compliance. Figure out which vendors have access to any personal information, review those contracts, and always double check the data use terms and conditions. Vendors should have ready-made data agreements (such as data processing agreements) in place, or be quickly ready to put such amendments in place to give your organization the legal contractual protections needed for data restrictions, as well as give you clear ways of mapping data.

7. Commit, plan, execute, and commit again.

Give you and your organization the right plan, the right tools/vendors, and the right commitment, otherwise compliance will be difficult, whether it's CCPA, GDPR or otherwise. Modifying an organization's mindset or behavior is typically a multi-step process that must persist and iterate continuously. Thinking that CCPA compliance will be a short-term project will set unrealistic expectations of those that need to participate and help execute on compliance. Picking vendors who are not ready also will frustrate an organization's compliance.

Take an organized and planned approach toward CCPA compliance. Start with data mapping – illustrating the collection, use, storage, and transfer of personal information. Developing processes for evaluating and responding to data access requests and training resources, employees and others will also take some time.

8. Should CCPA extend to your entire customer base?

A key choice an organization will have to make is whether CCPA should apply to all of its customers and individuals it reaches, not just those in California. It is ultimately an organization's decision. We at Episerver believe that each of our customers are very customer-centric, customer-facing and invests heavily in its relationships with consumers and business relations. It's for these reasons we encourage our customers to extend CCPA rights and protections to all US-based customers as a promotional, customer-friendly gesture. It's the same reason why Episerver enabled GDPR practices globally for all of it's software and services.

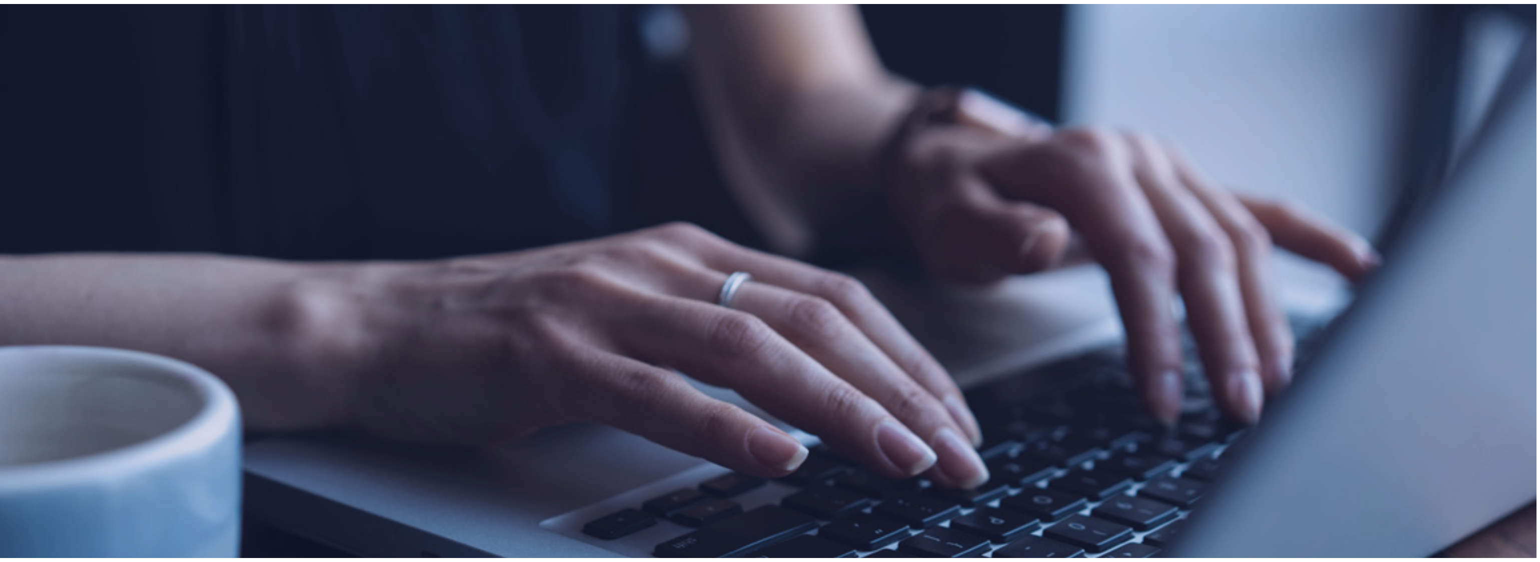
9. Train your resources.

CCPA has a requirement on training of resources who will be responsible for receiving and acting on consumer requests. Your team(s) need to understand the company's privacy program so they can help reduce risk for the business, both from the customer communications and process perspective.
Processes of responding efficiently to data access requests, deletion requests, and requests to opt-out of data sale are only as effective as the people and organizations that are executing them. These processes, as they do with GDPR, typically impact many operations and organizations within a business, thus employees and resources trained on personal information processes, policies and their own obligations will enable successful compliance.

10. CCPA compliance is not just a Legal and IT team compliance matter.

Of course there are aspects of CCPA for your Legal team, as well as your IT team for CCPA compliance. While data protection, tracking consent and the information within, deletion, and security do tend to be IT, compliance, legal and tech-oriented tasks, adherence to the CCPA is a company-wide commitment. Remember, it's often the marketing team's requirement for the data an organization is seeking to gather.

Assemble a committed team comprising of marketing, legal, compliance, business, and technology expertise at a minimum. They can assess the CCPA compliance strategy, implications and adherence to CCPA, and many similar legislation and regulations domestically in the US and globally expected in 2020.



Episerver and CCPA

Episerver's long, dedicated history to data protection and privacy by design has enabled thousands of customers to become GDPR compliant in short order and is a track record we are very proud of. As our continuing commitment develops, Episerver products and services can be key on an organization's journey to compliance with CCPA.

Please contact us with any CCPA questions on your digital engagement, website, and/or commerce site, and we will be happy to discuss how Episerver can aid your endeavours towards not just CCPA and GDPR compliance, but enable processes and tools to assist your future compliance and regulatory needs.

Peter Yeung
EPM Officer & General Counsel